



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

SEP 9 2004

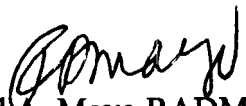
MEMORANDUM FOR DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE

SUBJECT: Request to Appoint a Service Headquarters Health Insurance Portability and Accountability Act of 1996 Security Official

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, administrative simplification provisions require the protection and privacy of individually identifiable health information. The HIPAA Security rule, signed in February 2003, mandates the standards for the integrity, confidentiality, and availability of electronically protected health information. Full compliance with its requirements must be met by April 21, 2005.

It is requested that a HIPAA Security Official be appointed for each Service. The person selected as the HIPAA Security Official must possess the requisite experience, knowledge, and authority to develop, implement, and monitor the security practices, policies, and procedures throughout the organization. The HIPAA Security Official will serve as a resource to military treatment facilities and dental treatment facilities (MTFs/DTFs) in the implementation of Department of Defense regulations and as a liaison to the TRICARE Regional Offices and TRICARE Management Activity (TMA). TMA will provide training and guidance for the person assigned.

The roles and responsibilities for the HIPAA Security Official are attached. Within two weeks of the date of this memorandum, please forward the name, phone number, and e-mail address of the appointed Security Official to Mr. Sam Jenkins, TMA Privacy Officer, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041, e-mail: Sam.Jenkins@tma.osd.mil, fax: 703-681-8845.


Richard A. Mayo RADM, MC, USN
Deputy Director

Attachment:
As stated

cc: Dr. Richard Guerin
Mr. Sam Jenkins

**SERVICE HEADQUARTERS
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
SECURITY OFFICIAL
ROLES AND RESPONSIBILITIES**

Organizational Need/Function: The Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, requires each covered entity, i.e., the TRICARE health plan and Medical Treatment Facilities and Dental Treatment Facilities (MTFs/DTFs), to assign HIPAA Security responsibilities. For Service specific policy and procedure development and implementation, a Service Headquarters level HIPAA Security Official in each Service is needed.

ROLES AND RESPONSIBILITIES

The HIPAA Security Official will perform functions to implement the HIPAA Security rule within the Service Headquarters:

- Ensure Service security policies and procedures comply with the HIPAA Security Rule and related Department of Defense (DoD) regulations.
- Ensure all staff complete initial HIPAA training using the web based TRICARE Management Activity (TMA) HIPAA training tool.
- Use the web based TMA HIPAA compliance tool to perform map and gap analyses.
- Provide an orientation and follow-on training to all employees.
- Initiate, facilitate and promote activities to foster information security awareness within the organization and related entities.
- Establish a mechanism within the organization for receiving, documenting, tracking, investigating, and taking action on all issues concerning the organization's security policies and procedures.
- Brief HIPAA Security implementation plan to Service Headquarters staff.
- Maintain current knowledge of applicable federal, DoD and state information security laws, accreditation standards, and DoD and Service regulations.
- Ensure that initial and periodic organizational risk assessments are conducted and that related ongoing compliance monitoring activities are in coordination with applicable Service directives and TMA. Report findings as required.
- Review the security features of new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply.
- Monitor entity operations and systems for security compliance. Report to management on the status of security compliance.

The HIPAA Security Official will serve as a Liaison:

- Serve as liaison between the Services, TMA and MTFs/DTFs on issues related to HIPAA Security implementation.
- Serve on TMA HIPAA Security Working Integrated Process Team (WIPT) and work groups as appropriate for further implementation of Security policies.
- In coordination with key personnel, oversee the development and implementation of the following plans and others as required: disaster plan, emergency mode operation plan, backup plan, physical security plan, personnel security plan, access policies, and others. Test and revise plans as necessary to ensure data integrity, confidentiality, and availability.
- Receive reports from the MTF/DTF level Security Officials of security breaches; assure appropriate action has been taken to minimize harm; conduct investigation of security breaches, and assure corrective actions have been taken.

The HIPAA Security Official will serve as an Administrator of the Military Health System HIPAA Security Program:

- Serve as a point of contact for Service HIPAA Security Rule compliance concerns, issues and policy questions as needed.
- Maintain current knowledge of all applicable state, DoD and federal requirements with regard to the security of electronic health information.
- Collaborate with other healthcare professionals to ensure appropriate security measures are in place to safeguard protected health information.
- Serve as the advocate for the patient relating to the security of health information.
- Conduct meetings with MTF/DTF Security Officials to ensure that information sharing and dissemination is consistent and in conformity with policy.